UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,833	11/16/2001	Hiroshi Koga	862.C2437	7585

			EXAMINER
5514	7590	02/21/2006	LANIER, BENJAMIN E

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/987,833	KOGA, HIROSHI
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>17 January 2006</u>.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-23 and 27-43</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-23 and 27-43</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>16 November 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

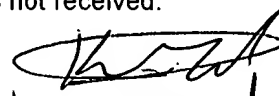11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1. ☒ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Kambiz Zand

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>2/2/2006</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail. Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

Response to Amendment

1.   Applicant's amendment filed 17 January 2006 amends claims 1, 2, 7-11, 13-19, 22, 23,

27-30, 32, cancels claims 24-26, and adds claims 33-43.

Response to Arguments

2.   Applicant's arguments filed 17 January 2006 have been fully considered but they are not

persuasive. Applicant's argument that the subject matter is statutory is not persuasive because as

stated previously the claim is drawn to a printer driver which is non-statutory subject matter

because it is a software object. MPEP 2106 clearly states:

> For products, the claim limitations will define discrete physical structures or materials.
> Product claims are claims that are directed to either machines, manufactures or
> compositions of matter. The discrete physical structures or materials may be comprised
> of hardware or a combination of hardware and software.

Therefore, because Applicant has failed claim the invention using hardware or a

combination of hardware and software, the limitations are considered to be non-statutory.

3.   Applicant's argument that the prior art does not disclose obtaining informaiton

identifying an application which has issued an instruction to print electronic data of a print object

and executing user authentication for approving or accounting for an output of the electronic data

based on the information identifying the application is not persuasive because Ota discloses that

there is an operation instructing means that is used to perform the print requests (Abstract &

Figure 1). This operation instructing means receives user authentication information to be

transmitted with the print request instruction (Abstract & Figure 1). Figure 2 shows the operation

instructing means as a job producing unit. Ota further discloses that this system operates using

the UNIX operating system (Col. 1, lines 21-22). In such an operating system, this operation

instructing means/job producing unit, which receives the user authentication information, for

inclusion in the print request instruction would meet the limitation of an application. The

operation instructing means/job producing unit when initialized by a user would spawn a print

process/print job, which would include the user authentication information and the data to be

printed amongst other things. These print processes/print jobs have a process id associated with

them so that the operating system task manager/schedule routine can differentiate between the

different processes. The process id would meet the limitation of informaiton identifying the

application.

4.   Applicant makes the same arguments with respect to the Kadowaki reference, which are

also not persuasive because Kadowaki also discloses that the print jobs are produced from an

operating system (Col. 27, lines 47-53). Therefore, the response to Applicant's arguments with

respect to Ota also apply to the arguments with respect to Kadowaki.

Claim Rejections - 35 USC § 101

5.   Claim 16 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-

statutory subject matter. The claim is drawn to a printer driver which is non-statutory subject

matter because it is a software object. The claim is a means plus function claim where the means

are not defined by the claims. The specification describes pure software embodiments of the

invention, see page 65, which is non-statutory subject matter. Amendments to the claims

specifically reciting hardware or, hardware and software are suggested.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7.   Claims 1, 2, 4, 7-9, 11, 13, 15, 22-27, 29, 33, 35, 39-43 are rejected under 35

U.S.C. 102(e) as being anticipated by Ota, U.S. Patent No. 6,163,383. Referring to claims 1, 7,

Ota discloses a method for providing printing security wherein user's on a client system requests

printing operations (Col. 3, lines 19-22). A print server receives the print request and extracts the

user information and authenticates the user identity (Col. 3, lines 33-36 & Col. 7, lines 26-31),

which meets the limitation of extracting informaiton related to an application and/or a document

for the print process as attribute information, executing user authentication based on the attribute

information. Ota discloses that there is an operation instructing means that is used to perform the

print requests (Abstract & Figure 1). This operation instructing means receives user

authentication information to be transmitted with the print request instruction (Abstract & Figure

1). Figure 2 shows the operation instructing means as a job producing unit. Ota further discloses

that this system operates using the UNIX operating system (Col. 1, lines 21-22). In such an

operating system, this operation instructing means/job producing unit, which receives the user

authentication information, for inclusion in the print request instruction would meet the

limitation of an application. The operation instructing means/job producing unit when initialized

by a user would spawn a print process/print job, which would include the user authentication

information and the data to be printed amongst other things. These print processes/print jobs

have a process id associated with them so that the operating system task manager/schedule

routine can differentiate between the different processes. The process id would meet the limitation of informaiton identifying the application.

Referring to claims 2, 8, Ota discloses that the user request includes an identification of a specific printing operation (Col. 3, lines 19-21), which would meet the limitation of extracting attribute information including the information identifying the application from the electronic data of the print object, the attribute information contains various kinds of document attribute informaiton including a application name.

Referring to claims 4, 11, Ota discloses that the user request includes the user name (Col. 3, line 23), which meets the limitation of application user.

Referring to claims 9, 13, Ota discloses that the authentication system contains a client computer, printer server, and printer (Figure 2), which meets the limitation of a client computer or print server which is installed with a printer driver, a server for managing a network, and a printer for executing the print process, which are connected via a network. The job receiving unit of the printer server extracts the user informaiton for authentication (Col. 7, lines 30-31), which meets the limitation of obtaining means and extraction means is included in the printer driver. The printer server also contains a user verification unit (Figure 2), which meets the limitation of user authentication means is included in the server.

Referring to claim 15, Ota discloses a method for providing printing security wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print server receives the print request and extracts the user information and authenticates the user identity (Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of means of receiving information related to an application and/or a document for the print process as attribute

information, means for extracting information required for user authentication from the attribute

information. In high-level authentication mode, the printer server sends the request and user

information to an authentication server for authentication and then notifies the printer server of

the result (Col. 3, lines 50-56), which meets the limitation of means of sending a user

authentication request appended with the extracted information to a server via a network. If

authenticated the user's print request is completed by the printer (Col. 3, lines 35-38), which

meets the limitation of means of, when user authentication has succeeded, controlling a printer to

execute the print process. Ota discloses that there is an operation instructing means that is used to

perform the print requests (Abstract & Figure 1). This operation instructing means receives user

authentication information to be transmitted with the print request instruction (Abstract & Figure

1). Figure 2 shows the operation instructing means as a job producing unit. Ota further discloses

that this system operates using the UNIX operating system (Col. 1, lines 21-22). In such an

operating system, this operation instructing means/job producing unit, which receives the user

authentication information, for inclusion in the print request instruction would meet the

limitation of an application. The operation instructing means/job producing unit when initialized

by a user would spawn a print process/print job, which would include the user authentication

information and the data to be printed amongst other things. These print processes/print jobs

have a process id associated with them so that the operating system task manager/schedule

routine can differentiate between the different processes. The process id would meet the

limitation of informaiton identifying the application.

Referring to claims 16, 25, Ota discloses a method for providing printing security

wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print

server receives the print request and extracts the user information and authenticates the user

identity (Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of means of

receiving information related to an application and/or a document for the print process as

attribute information, means for extracting information required for user authentication from the

attribute information. The user request includes an identification of a specific printing operation

(Col. 3, lines 19-21) and if authenticated the user's print request is completed by the printer (Col.

3, lines 35-38), which meets the limitation of means of sending print information appended with

the extracted information to a printer. Ota discloses that there is an operation instructing means

that is used to perform the print requests (Abstract & Figure 1). This operation instructing means

receives user authentication information to be transmitted with the print request instruction

(Abstract & Figure 1). Figure 2 shows the operation instructing means as a job producing unit.

Ota further discloses that this system operates using the UNIX operating system (Col. 1, lines

21-22). In such an operating system, this operation instructing means/job producing unit, which

receives the user authentication information, for inclusion in the print request instruction would

meet the limitation of an application. The operation instructing means/job producing unit when

initialized by a user would spawn a print process/print job, which would include the user

authentication information and the data to be printed amongst other things. These print

processes/print jobs have a process id associated with them so that the operating system task

manager/schedule routine can differentiate between the different processes. The process id would

meet the limitation of informaiton identifying the application.

Referring to claim 17, Ota discloses a method for providing printing security wherein

user's on a client system requests printing operations (Col. 3, lines 19-22). A print server

receives the print request and extracts the user information and authenticates the user identity

(Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of means of receiving

information, which is required for user authentication and is extracted from attribute information

related to an application and/or a document for the print process, from a printer driver via a

network. The print server contains an authentication table (Figure 4) that contains pre-registered

information about each user, including the operations for which they have access (Col. 8, line 56

– Col. 9, line 3 & Figures 3B, 4), which meets the limitation of checking a user authentication

result by comparing the extracted information with user authentication information which is

registered in advance. The results of the authentication process are returned to the client (Col. 10,

lines 56-57), which meets the limitation of means of returning the user authentication result to

the printer driver via the network. Ota discloses that there is an operation instructing means that

is used to perform the print requests (Abstract & Figure 1). This operation instructing means

receives user authentication information to be transmitted with the print request instruction

(Abstract & Figure 1). Figure 2 shows the operation instructing means as a job producing unit.

Ota further discloses that this system operates using the UNIX operating system (Col. 1, lines

21-22). In such an operating system, this operation instructing means/job producing unit, which

receives the user authentication information, for inclusion in the print request instruction would

meet the limitation of an application. The operation instructing means/job producing unit when

initialized by a user would spawn a print process/print job, which would include the user

authentication information and the data to be printed amongst other things. These print

processes/print jobs have a process id associated with them so that the operating system task

manager/schedule routine can differentiate between the different processes. The process id would

meet the limitation of informaiton identifying the application.

Referring to claim 22, Ota discloses that the user request includes the user name (Col. 3,

line 23), which meets the limitation of application user.

Referring to claims 23, 26, Ota discloses a method for providing printing security

wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print

server receives the print request and extracts the user information and authenticates the user

identity (Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of means of

receiving information, which is required for user authentication and is extracted from attribute

information related to an application and/or a document for the print process, from a printer

driver together with print information, means of inputting user authentication information. The

print server contains an authentication table (Figure 4) that contains pre-registered information

about each user, including the operations for which they have access (Col. 8, line 56 – Col. 9,

line 3 & Figures 3B, 4), which meets the limitation of means of executing user authentication on

the basis of a comparison result of the information required for user authentication and the input

information. Ota discloses that there is an operation instructing means that is used to perform the

print requests (Abstract & Figure 1). This operation instructing means receives user

authentication information to be transmitted with the print request instruction (Abstract & Figure

1). Figure 2 shows the operation instructing means as a job producing unit. Ota further discloses

that this system operates using the UNIX operating system (Col. 1, lines 21-22). In such an

operating system, this operation instructing means/job producing unit, which receives the user

authentication information, for inclusion in the print request instruction would meet the

limitation of an application. The operation instructing means/job producing unit when initialized

by a user would spawn a print process/print job, which would include the user authentication

information and the data to be printed amongst other things. These print processes/print jobs

have a process id associated with them so that the operating system task manager/schedule

routine can differentiate between the different processes. The process id would meet the

limitation of informaiton identifying the application.

Referring to claim 27, Ota discloses a method for providing printing security wherein

user's on a client system requests printing operations (Col. 3, lines 19-22). A print server

receives the print request and extracts the user information and authenticates the user identity

(Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of extracting means of

extracting information related to an application and/or a document for the print process as

attribute information. In high-level authentication mode, the printer server sends the request and

user information to an authentication server for authentication and then notifies the printer server

of the result (Col. 3, lines 50-56), which meets the limitation of means output means of

outputting the attribute information extracted by said extracting means to said external

information processing apparatus using the attribute information for a user authentication for the

print process. Ota discloses that there is an operation instructing means that is used to perform

the print requests (Abstract & Figure 1). This operation instructing means receives user

authentication information to be transmitted with the print request instruction (Abstract & Figure

1). Figure 2 shows the operation instructing means as a job producing unit. Ota further discloses

that this system operates using the UNIX operating system (Col. 1, lines 21-22). In such an

operating system, this operation instructing means/job producing unit, which receives the user

authentication information, for inclusion in the print request instruction would meet the

limitation of an application. The operation instructing means/job producing unit when initialized

by a user would spawn a print process/print job, which would include the user authentication

information and the data to be printed amongst other things. These print processes/print jobs

have a process id associated with them so that the operating system task manager/schedule

routine can differentiate between the different processes. The process id would meet the

limitation of informaiton identifying the application.

Referring to claim 29, Ota discloses that the user request includes an identification of a

specific printing operation (Col. 3, lines 19-21), which would meet the limitation of information

further contains an application name indicating an application to be used.

Referring to claims 33, 41, Ota discloses a method for providing printing security

wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print

server receives the print request and extracts the user information and authenticates the user

identity (Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of an extracting

step of extracting information identifying an application which has issued an instruction to print

electronic data of a print object. In high-level authentication mode, the printer server sends the

request and user information to an authentication server for authentication and then notifies the

printer server of the result (Col. 3, lines 50-56), which meets the limitation of an output step of

outputting the information extracted by said extracting step to said external information

processing apparatus to use the information for a user authentication for the print process. Ota

discloses that there is an operation instructing means that is used to perform the print requests

(Abstract & Figure 1). This operation instructing means receives user authentication information

to be transmitted with the print request instruction (Abstract & Figure 1). Figure 2 shows the

operation instructing means as a job producing unit. Ota further discloses that this system

operates using the UNIX operating system (Col. 1, lines 21-22). In such an operating system, this

operation instructing means/job producing unit, which receives the user authentication

information, for inclusion in the print request instruction would meet the limitation of an

application. The operation instructing means/job producing unit when initialized by a user would

spawn a print process/print job, which would include the user authentication information and the

data to be printed amongst other things. These print processes/print jobs have a process id

associated with them so that the operating system task manager/schedule routine can differentiate

between the different processes. The process id would meet the limitation of informaiton

identifying the application.

Referring to claim 35, Ota discloses that the user request includes an identification of a

specific printing operation (Col. 3, lines 19-21), which would meet the limitation of the attribute

information contains various kinds of document attribute informaiton including a application

name.

Referring to claims 39, 42, Ota discloses a method for providing printing security

wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print

server receives the print request and extracts the user information and authenticates the user

identity (Col. 3, lines 33-36 & Col. 7, lines 26-31). In high-level authentication mode, the printer

server sends the request and user information to an authentication server for authentication and

then notifies the printer server of the result (Col. 3, lines 50-56), which meets the limitation of a

receiving step of receiving information identifying an application which has issued an instruction

to print electronic data of a print object from a printer driver via a network, a checking step of

checking a user authentication result by comparing the received information with user

authentication information which is registered in advance, a returning step of returning the user

authentication result to the printer driver via the network. Ota discloses that there is an operation

instructing means that is used to perform the print requests (Abstract & Figure 1). This operation

instructing means receives user authentication information to be transmitted with the print

request instruction (Abstract & Figure 1). Figure 2 shows the operation instructing means as a

job producing unit. Ota further discloses that this system operates using the UNIX operating

system (Col. 1, lines 21-22). In such an operating system, this operation instructing means/job

producing unit, which receives the user authentication information, for inclusion in the print

request instruction would meet the limitation of an application. The operation instructing

means/job producing unit when initialized by a user would spawn a print process/print job,

which would include the user authentication information and the data to be printed amongst other

things. These print processes/print jobs have a process id associated with them so that the

operating system task manager/schedule routine can differentiate between the different

processes. The process id would meet the limitation of informaiton identifying the application.

Referring to claims 40, 43, Ota discloses a method for providing printing security

wherein user's on a client system requests printing operations (Col. 3, lines 19-22). A print

server receives the print request and extracts the user information and authenticates the user

identity (Col. 3, lines 33-36 & Col. 7, lines 26-31), which meets the limitation of an inputting

step of inputting user authentication information. In high-level authentication mode, the printer

server sends the request and user information to an authentication server for authentication and

then notifies the printer server of the result (Col. 3, lines 50-56), which meets the limitation of a receiving step of receiving information identifying an application which has issued an instruction to perform the print process from a printer driver together with print informaiton, an execution step of executing user authentication on the basis of a comparison result of the information identifying the application and the input user authentication information. Ota discloses that there is an operation instructing means that is used to perform the print requests (Abstract & Figure 1). This operation instructing means receives user authentication information to be transmitted with the print request instruction (Abstract & Figure 1). Figure 2 shows the operation instructing means as a job producing unit. Ota further discloses that this system operates using the UNIX operating system (Col. 1, lines 21-22). In such an operating system, this operation instructing means/job producing unit, which receives the user authentication information, for inclusion in the print request instruction would meet the limitation of an application. The operation instructing means/job producing unit when initialized by a user would spawn a print process/print job, which would include the user authentication information and the data to be printed amongst other things. These print processes/print jobs have a process id associated with them so that the operating system task manager/schedule routine can differentiate between the different processes. The process id would meet the limitation of informaiton identifying the application.

8.   Claims 1-14, 16-23, 25-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Kadowaki, U.S. Patent No. 6,313,921. Referring to claims 1, 7, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print

jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server

extracts personalizing information stored for each machine type and for each user and then sends

this information to the printer (Col. 13, lines 9-15), which meets the limitation of extracting

information related to an application and/or a document for the print process as attribute

information. The printer then checks the personalizing information to make sure that the user has

not exceeding their printing privileges (Col. 14, lines 31-38), which meets the limitation of

executing user authentication based on the attribute information. The explanation of how

operating systems issuing print jobs meet the new claim limitations, given with respect to the Ota

reference, is also applicable to the Kadowaki reference because Kadowaki also discloses that the

print jobs are produced from an operating system (Col. 27, lines 47-53).

Referring to claims 2, 8, Kadowaki discloses that the document name is included in the

print job request (Col. 10, lines 51-53).

Referring to claims 3, 5, 10, 12, Kadowaki discloses that the cost for the print job is

calculated for the user (Col. 10, lines 30-44), which meets the limitation of when user

authentication has succeeded and a print process is executed, an accounting process of

expendables associated with the document print process, and for the user of the application, for

each user or each department of a group to which the user belongs.

Referring to claims 4, 11, Kadowaki discloses that the print job requests contain a user ID

(Col. 13, line 10), which meets the limitation of an application user.

Referring to claims 6, 14, Kadowaki discloses that the user ID contains a password (Col.

3, line 10).

Referring to claims 9, 13, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56), which meets the limitation of a print server which is installed with a printer driver and a printer for executing the print process connected via a network. Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65), which meets the limitation of a client computer connected via a network. Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of obtaining means and extraction means included in the printer driver. The personalizing server contains authentication means for authentication the print job request (Col. 18, lines 38- 66).

Referring to claim 16, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of means for receiving informaiton related to an application and/or a document for the print process as attribute informaiton, means of extracting information required for user authentication from the attribute information, means of sending print information appended with the extracted information to a printer. The explanation of how operating systems issuing print jobs meet the new claim limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference because

Kadowaki also discloses that the print jobs are produced from an operating system (Col. 27, lines 47-53).

Referring to claim 17, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of means of receiving information, which is required for user authentication and is extracted from attribute information related to an application and/or a document for the print process, from a printer driver via a network. The printer then checks the personalizing information to make sure that the user has not exceeding their printing privileges (Col. 14, lines 31-38), which meets the limitation of means of checking a user authentication result by comparing the extracted information with user authentication informaiton which is registered in advance. The printer returns a report to the user about the print job (Col. 14, lines 19-38), which meets the limitation of means of returning the user authentication result to the printer driver via the network. The explanation of how operating systems issuing print jobs meet the new claim limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference because Kadowaki also discloses that the print jobs are produced from an operating system (Col. 27, lines 47-53).

Referring to claims 18, 19, Kadowaki discloses that the cost for the print job is calculated for the user (Col. 10, lines 30-44), which meets the limitation of when user authentication has succeeded and a print process is executed, an accounting process of expendables associated with

the document print process, and for the user of the application, for each user or each department

of a group to which the user belongs. The print job requests also contain a group ID (Col. 13,

lines 34), which would meet the limitation of department of the group to which the user belongs.

Referring to claim 20, Kadowaki discloses that the printer updates the stored information

about the user. For instance, the printer will update the amount of pages the user can print after

each print job (Col. 13, lines 41-55 & Col. 14, lines 31-38), which meets the limitation of means

of registering and holding various kinds of attribute information of departments, affiliations,

individuals, print accounting states, associated with clients, users, and groups who make a

document print process, means of updating use states of a printer used in a print process for

respective departments, affiliations, and individuals.

Referring to claims 21, 22, Kadowaki discloses that the personalizing server contains

authentication means for authentication the print job request, and that the user ID and password

are items that are authenticated (Col. 18, lines 38- 66), which meets the limitation of attribute

information contains various kinds of document attribute information including password and

said checking means comprises means of executing department authentication of a user or the

like by comparing a password registered in said server on the basis of various kinds of document

attribute information, said checking means comprises means of granting permission of use of the

application on the basis of the application attribute information.

Referring to claim 23, Kadowaki discloses a printing system wherein a printer and a

personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are

also connected to the network for generating and sending print jobs to the printer (Col. 6, lines

63-65). Once the print job is received, the personalization server extracts personalizing

information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of means of receiving information, which is required for user authentication and is extracted from attribute information related to an application and/or a document for the print process, from a printer driver together with print information, means of inputting user authentication information. The printer then checks the personalizing information to make sure that the user has not exceeding their printing privileges (Col. 14, lines 31-38). The printer returns a report to the user about the print job (Col. 14, lines 19-38), which meets the limitation of means of executing user authentication on the basis of a comparison result of the information required for user authentication and the input informaiton. The explanation of how operating systems issuing print jobs meet the new claim limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference because Kadowaki also discloses that the print jobs are produced from an operating system (Col. 27, lines 47-53).

Referring to claim 25, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of means of receiving information related to an application and/or a document for the print process as attribute information, extracting information required for user authentication from the attribute information, sending print information appended with the extracted information to a printer.

Referring to claim 27, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of extracting means of extracting information related to an application and/or a document for the print process as attribute information, and output means of outputting the attribute information extracted by said extracting means to said external informaiton processing apparatus using the attribute information for a user authentication for the print process. The explanation of how operating systems issuing print jobs meet the new claim limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference because Kadowaki also discloses that the print jobs are produced from an operating system (Col. 27, lines 47-53).

Referring to claim 28, Kadowaki discloses that the document name is included in the print job request (Col. 10, lines 51-53).

Referring to claim 29, Kadowaki discloses that the print job request contains a function name that indicates which function to use (Col. 13, lines 15-21 & Col. 14, lines 11-15), which meets the limitation of an application name.

Referring to claims 30-32, Kadowaki discloses that once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15) through the network (Col. 7, lines 1-2 & Figure 1). At the printer the external interface, connected to a CPU, receive

the print job (Col. 7, lines 2-3 & Figure 1), which meets the limitation of extracting means

extracts the attribute informaiton by calling a printer driver module and API provided between

OS and the printer driver module and causing OS to operate a document in said apparatus, API is

provided in the printer driver module, extracting means calls said API in response to a print

instructor inputted from the application. The CPU includes an Operating System that performs

the processes in accordance with designations of the program codes (Col. 27, lines 47-52).

   Referring to claims 33, 41, Kadowaki discloses a printing system wherein a printer and a

personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are

also connected to the network for generating and sending print jobs to the printer (Col. 6, lines

63-65). Once the print job is received, the personalization server extracts personalizing

information stored for each machine type and for each user and then sends this information to the

printer (Col. 13, lines 9-15), which meets the limitation of an extracting step of extracting

information identifying an application which has issued an instruction to print electronic data of

a print object. The printer then checks the personalizing information to make sure that the user

has not exceeding their printing privileges (Col. 14, lines 31-38), which meets the limitation of

an output step of outputting the information extracted by said extracting step to said external

informaiton processing apparatus to use the informaiton for a user authentication for the print

process. The explanation of how operating systems issuing print jobs meet the new claim

limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference

because Kadowaki also discloses that the print jobs are produced from an operating system (Col.

27, lines 47-53).

Referring to claim 34, Kadowaki discloses that the document name is included in the print job request (Col. 10, lines 51-53).

Referring to claim 35, Kadowaki discloses that the print job request contains a function name that indicates which function to use (Col. 13, lines 15-21 & Col. 14, lines 11-15), which meets the limitation of an application name.

Referring to claims 36-38, Kadowaki discloses that once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15) through the network (Col. 7, lines 1-2 & Figure 1). At the printer the external interface, connected to a CPU, receive the print job (Col. 7, lines 2-3 & Figure 1), which meets the limitation of extracting means extracts the attribute informaiton by calling a printer driver module and API provided between OS and the printer driver module and causing OS to operate a document in said apparatus, API is provided in the printer driver module, extracting means calls said API in response to a print instructor inputted from the application. The CPU includes an Operating System that performs the processes in accordance with designations of the program codes (Col. 27, lines 47-52).

Referring to claims 39, 42, Kadowaki discloses a printing system wherein a printer and a personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are also connected to the network for generating and sending print jobs to the printer (Col. 6, lines 63-65). Once the print job is received, the personalization server extracts personalizing information stored for each machine type and for each user and then sends this information to the printer (Col. 13, lines 9-15), which meets the limitation of a receiving step of receiving information identifying an application which has issued an instruction to print electronic data of

a print object from a printer driver via a network. The printer then checks the personalizing

information to make sure that the user has not exceeding their printing privileges (Col. 14, lines

31-38), which meets the limitation of a checking step of checking a user authentication result by

comparing the received information with user authentication information which is registered in

advance, a returning step of returning the user authentication result to the printer driver via the

network. The explanation of how operating systems issuing print jobs meet the new claim

limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference

because Kadowaki also discloses that the print jobs are produced from an operating system (Col.

27, lines 47-53).

Referring to claims 40, 43, Kadowaki discloses a printing system wherein a printer and a

personalizing server are connected through a network (Col. 6, lines 55-56). Client computers are

also connected to the network for generating and sending print jobs to the printer (Col. 6, lines

63-65). Once the print job is received, the personalization server extracts personalizing

information stored for each machine type and for each user and then sends this information to the

printer (Col. 13, lines 9-15), which meets the limitation of a receiving step of receiving

information identifying an application which has issued an instruction to perform the print

process from a printer driver together with print information, an inputting step of inputting user

authentication information. The printer then checks the personalizing information to make sure

that the user has not exceeding their printing privileges (Col. 14, lines 31-38), which meets the

limitation of an executing step of executing user authentication on the basis of a comparison

result of the information identifying the application and the input user authentication

information. The explanation of how operating systems issuing print jobs meet the new claim

limitations, given with respect to the Ota reference, is also applicable to the Kadowaki reference

because Kadowaki also discloses that the print jobs are produced from an operating system (Col.

27, lines 47-53).

Conclusion

9.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

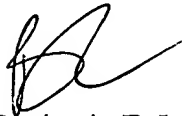Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

10.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

Kambiz Zand

Primary Examiner